HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN ĐỨC HẢI

NGHIÊN CỨU CÔNG NGHỆ XÁC THỰC NGƯỜI DÙNG ỨNG DỤNG TRONG QUẢN LÝ TRUY CẬP DỊCH VỤ ĐIỆN TOÁN ĐÁM MÂY

Chuyên ngành: Hệ thống thông tin

Mã số: 60.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2013

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. Hoàng Lê Minh

Phản biện 1: ……

Phản biện 2: ..……..

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng ..... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

I. PHẦN MỞ ĐẦU

1. Lý do chọn đề tài

Với sự phát triển của mạng Internet hiện nay, các doanh nghiệp nhanh chóng nhận thấy lợi ích của việc sử dụng mạng Internet để mở rộng thêm mạng doanh nghiệp bao gồm cả các đối tác, nhà cung cấp và nhất là thông qua Internet, các doanh nghiệp có thể cung cấp các dịch vụ của mình đến với khách hàng thông qua các ứng dụng web.

Tuy nhiên, với việc mở rộng mạng doanh nghiệp đến nhiều đối tượng, doanh nghiệp bắt buộc phải cung cấp dữ liệu thông tin của mình cho các đối tượng đó. Do vậy, vấn đề đặt ra ở đây là khả năng đảm bảo an ninh mạng là một trong những yếu tố sống còn cho một doanh nghiệp khi áp dụng mô hình thương mại điện tử. An ninh mạng bao gồm rất nhiều các khía cạnh khác nhau.

Ngày nay với sự ra đời của Điện toán đám mây (Cloud Computing): có thể hiểu là mô hình điện toán sử dụng các công nghệ phần mềm, khoa học máy tính,… được phát triển trên hạ tầng mạng máy tính và Internet, để tạo ra một "đám mây" cung cấp từ cơ sở hạ tầng, nơi lưu trữ dữ liệu cho đến các dịch vụ sẵn sàng, nhanh chóng cho mọi cơ quan, tổ chức doanh nghiệp và người dùng đầu cuối theo yêu cầu. Mô hình dịch vụ đám mây, người dùng không phải quan tâm đến kỹ năng cài đặt, triển khai và ứng dụng phần mềm, các yêu cầu về cở sở hạ tầng truyền thông, mạng máy tính và Internet để truy cập các dịch vụ. Cloud Computing giải quyết các vấn đề tối ưu hóa lưu trữ, ảo hóa máy chủ, cơ sở hạ tầng mạng. Ảo hóa tính toán, sử dụng các siêu máy tính (Super-Computer) để xử lý tính toán và công nghệ tính toán song song, phân tán, tính toán lưới.

Một trong những khía cạnh được quan tâm nhất khi xem xét một hệ thống an ninh mạng trong điện toán đám mây đó là công nghệ xác thực. Vì vậy, em đã lựa chọn đề tài: "Nghiên cứu công nghệ xác thực người dùng ứng dụng trong quản lý truy cập dịch vụ điện toán đám mây" làm luận văn tốt nghiệp của mình.

2. Mục đích nghiên cứu

- Tìm hiểu về điện toán đám mây.
- Tìm hiểu về dịch vụ điện toán đám mây.
- Nghiên cứu mô hình xác thực hai yếu tố trong điện toán đám mây.
- Xây dựng phần mềm minh họa quá trình xác thực hai yếu tố trong điện toán đám mây rồng thông minh iDragon bằng việc sử dụng giải pháp nguồn mở Google Authenticator cài

đặt trên các điện thoại thông minh hoặc máy tính bảng sử dụng hệ diều hành Android hay iOS. Google Authenticator đã có sẵn trên thư viện app của Android hay iOS.

3. Đối tượng và phạm vi nghiên cứu

- Các loại hình điện toán đám mây.
- Tập trung nghiên cứu công nghệ Two factor Authentication.

4. Phương pháp nghiên cứu

- Phân tích, nghiên cứu tài liệu và tổng hợp tài liệu.
- Phân tích, đánh giá các kỹ thuật xác thực.
- Phương pháp thực nghiệm bằng cách lập trình.

II. PHẦN NỘI DUNG

Nội dung nghiên cứu được trình bày trong các chương:

Chương 1: CÁC CÔNG NGHỆ XÁC THỰC TRUYỀN THỐNG, PHÂN TÍCH ƯU NHƯỢC ĐIỂM

1.1. Tổng quan về xác thực

1.1.1. Định nghĩa xác thực

Các nhà quản trị mạng ngày nay phải điều khiển việc truy cập cũng như giám sát thông tin mà người dùng đầu cuối đang thao tác. Những việc làm đó có thể đưa đến thành công hay thất bại của công ty. Với ý tưởng đó, AAA [3] là cách thức tốt nhất để giám sát những gì mà người dùng đầu cuối có thể làm trên mạng.

AAA [3] có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Ta có thể bật các dịch vụ AAA [3] trên router, switch, firewall, các thiết bị VPN, server, …

Các dịch vụ AAA [3] được chia thành ba phần:

+ Xác thực (Authentication): Xác thực dùng để nhận dạng (identify) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong AAA Server.
+ Thẩm quyền (Authorization): Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức.
+ Tính cước (Accounting): Accounting cho phép nhà quản trị có thể thu thập thông tin như thời gian bắt đầu, thời gian kết thúc người dùng truy cập vào hệ thống,

các câu lệnh đã thực thi, thống kê lưu lượng, việc sử dụng tài nguyên và sau đó lưu trữ thông tin trong hệ thống cơ sở dữ liệu quan hệ.

Như vậy, xác thực nằm ở vị trí đầu tiên trong cách thức để giám sát những gì mà người dùng đầu cuối có thể làm trên mạng.

Xác thực (tiếng Anh: Authentication - xuất phát từ Authentic có nghĩa là "thật", "thực","đích thực" hoặc "chính cống") là một hành động nhằm xác lập hoặc chứng thực một người nào đó (hay một cái gì đó) đáng tin cậy, có nghĩa là những lời khai báo do người đó đưa ra hoặc về cái đó là sự thật.

1.1.2. Vấn đề xác thực người dùng và tầm quan trọng của nó

Hệ thống xác thực người dùng đóng vai trò hết sức to lớn trong việc bảo mật thông tin của người dùng trong thời kì hiện đại hoá ngày nay. Các người sử dụng đã bao giờ đặt ra câu hỏi nếu không có hệ thống xác thực người dùng thì làm sao giữ an toàn được những thông tin bí mật hoặc làm sao quản lý được các bí mật trong kinh doanh, thương mại và tài khoản ở ngân hàng hoặc những nguồn tài nguyên được chia sẻ ở trên mạng từ một máy chủ? Với tên và mật khẩu chính xác người sử dụng có thể truy cập vào các tệp tin, thư điện tử, tài khoản của người sử dụng ở ngân hàng hay những thông tin cá nhân của người sử dụng …Mà người sử dụng không muốn một người dùng nào khác biết được. Vì vậy có thể nói lợi ích do hệ thống này mang lại là rất lớn đối với cuộc sống hiện đại ngày nay.

1.2. Phân tích, đánh giá các công nghệ xác thực truyền thống

1.2.1. Xác thực dựa trên username/password

1.2.1.1. Mô tả

Nhằm kiểm soát quyền truy cập ở mức hệ thống. Mỗi người sử dụng muốn vào được mạng để sử dụng tài nguyên đều phải đăng ký tên và mật khẩu. Người quản trị mạng có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của người sử dụng khác tuỳ theo không gian và thời gian.

1.2.1.2. Cơ chế xác thực bằng Username/password

Khi người dùng muốn đăng nhập và sử dụng tài nguyên hệ thống thì phải đăng nhập bằng cách nhập tên và mật khẩu của mình. Trước hết, hệ thống sẽ đối chiếu tên truy nhập của người dùng đưa vào với cơ sở dữ liệu tên người dùng, nếu tồn tại tên người dùng như vậy thì hệ thống tiếp tục đối chiếu mật khẩu được đưa vào tương ứng với tên truy nhập

trong cơ sở dữ liệu. Qua hai lần đối chiếu nếu thỏa mãn thì người đăng nhập là người dùng hợp lệ của hệ thống.

1.2.1.3. Ưu điểm

- Thiết kế và sử dụng đơn giản, tốn ít tài nguyên.
- Người dùng dễ hiểu và dễ sử dụng.
- Chi phí để thực hiện giải pháp này là rẻ so với các giải pháp khác. Nó không phụ thuộc vào các thiết bị phần cứng mà chỉ dựa trên phần mềm.
- Giải pháp này có khả năng làm việc trên mọi hệ điều hành. Do đó, việc thực hiện giải pháp này khá dễ dàng và không tốn kém.
- Đơn giản, dễ sử dụng.
- Không cần thêm bất cứ một phần mềm hoặc phần cứng nào.

1.2.1.4. Nhược điểm

- Dễ bị giả mạo: chỉ cần biết được mật khẩu của ai đó, hacker hoàn toàn có thể mạo danh người đó để thực hiện các giao dịch trên mạng hoặc đăng nhập vào hệ thống để tiến hành phá hoại hay đánh cắp thông tin.
- Dễ bị đánh cắp: một mật khẩu thông thường là được dùng nhiều lần, do vậy chỉ cần những phần mềm đơn giản (có thể tải được một cách dễ dàng từ Internet), một hacker có thể chặn bắt được các gói tin trên mạng và lấy cắp được mật khẩu người sử dụng.
- Quản lý khó khăn: với nhiều hệ thống, người sử dụng phải sử dụng nhiều mật khẩu, do vậy, vấn đề quản lý mật khẩu trở nên phức tạp.
- Chi phí cao: trong một mạng doanh nghiệp lớn, sẽ có rất nhiều yêu cầu tới bộ phận hỗ trợ kỹ thuật về các vấn đề liên quan đến mật khẩu và hầu hết trong số đó sẽ là do người sử dụng quên mật khẩu, mật khẩu bị hết hạn sử dụng,...

Kết luận:

Với tất cả những nhược điểm trên, chúng ta có thể thấy rằng xác thực bằng mật khẩu không thể đảm bảo được an toàn và độ tin cậy nhất là trong những lĩnh vực nhậy cảm như ngành ngân hàng, tài chính, bưu điện, dịch vụ y tế,... nơi mà những thông tin cần phải được giữ bí mật tuyệt đối. Người sử dụng thậm chí có thể khởi kiện những tổ chức cung cấp dịch vụ do những thông tin cá nhân của họ bị tiết lộ. Trong một hội thảo về an ninh mạng do hãng RSA tổ chức vào tháng 2 năm 2004, ngay cả chủ tịch Microsoft, Bill Gate cũng đã phát biểu là xác thực người dùng bằng mật khẩu hiện nay là không an toàn. Vì vậy, nếu chỉ sử dụng username/password sẽ không an toàn trong điện toán đám mây.

1.2.2. Xác thực dựa trên vật mang tin

1.2.2.1. Thẻ thông minh

Thẻ thông minh (Smart card) là một thiết bị an toàn, tuy nhiên vẫn có thể bị hư hỏng. Có rất ít cuộc tấn công vào thẻ thông minh và chi phí để thực hiện các cuộc tấn công này rất cao. Mặc dù vậy, chi phí đầu tư cho thẻ thông minh cũng rất lớn và vẫn còn nguy cơ rủi ro. Cho nên, nếu chỉ dùng thẻ thông minh sẽ không thích hợp để xác thực trong điện toán đám mây.

1.2.2.1.1. Cấu tạo của thẻ thông minh

Về cơ bản, thẻ thông minh bao gồm 3 bộ phận. Thẻ nhựa là bộ phận quan trọng nhất có kích thước 85,6x53,98x0,8mm. Một mạch in và một con chip vi mạch được gắn vào trên thẻ. Tính năng của thẻ thông minh phụ thuộc vào loại con chip vi mạch gắn trên thẻ. Con chip vi mạch này thường bao gồm một bộ vi xử lý, một bộ nhớ ROM, một bộ nhớ RAM và một bộ nhớ EEPROM.

1.2.2.1.2. Cơ chế hoạt động

Người sử dụng đưa thẻ vào đầu đọc theo đúng chiều quy định. Sau đó nhập mã số PIN để xác nhận quyền sử dụng thẻ. Số PIN không nằm trên thẻ mà được mã hoá trong một cơ sở dữ liệu.

1.2.2.1.3. Kỹ thuật tấn công thẻ thông minh

Cách thứ nhất: Do tất cả các thông tin quan trọng của thẻ thông minh được lưu giữ trong bộ nhớ EEPROM, trong khi đó bộ nhớ này có thể bị ảnh hưởng do những thay đổi về điện áp hoặc nhiệt độ nên những thông tin quan trọng có thể bị đánh cắp bằng việc tăng hoặc giảm điện áp ở bộ phận vi điều khiển.

Cách thứ hai: Bọn tội phạm tách rời con chip vi mạch ra khỏi tấm thẻ nhựa và tấn công trực tiếp vào con chip.

Kết luận:

Thẻ thông minh dùng để xác nhận khách hàng là một trong những cách an ninh nhất, có thể dùng trong những ứng dụng như giao dịch ngân hàng qua internet, nhưng mức độ an ninh không thể đảm bảo tuyệt đối. Có rất nhiều ngân hàng sử dụng thẻ thông minh để thực hiện các giao dịch. Tuy nhiên, muốn đảm bảo an toàn phải dùng chung một thẻ thông minh với một máy đọc thẻ không nối mạng nhằm giải quyết những vấn đề xấu xảy ra. Khách hàng nhập một thông tin đánh giá từ trang web của ngân hàng, PIN của họ, và tổng số tiền

giao dịch vào một máy đọc thẻ, máy đọc thẻ sẽ trả lại một chữ ký 8 chữ số. Chữ ký này sẽ được khách hàng nhập bằng tay vào PC và được kiểm chứng bởi ngân hàng.

Thẻ thông minh là một thiết bị an toàn, tuy nhiên vẫn có thể bị hư hỏng. Vẫn có những cuộc tấn công vào thẻ thông minh, trong trường hợp giao dịch ngân hàng qua internet, nếu PC bị nhiễm bởi các phần mềm xấu (Ví dụ như Trojan. Silentbanker), mô hình an ninh sẽ bị phá vỡ. Phần mềm xấu có thể viết đè lên thông tin (cả thông tin đầu vào từ bàn phím và thông tin đầu ra màn hình) giữa khách hàng và ngân hàng. Nó có thể sẽ sửa đổi giao dịch mà khách hàng không biết.

Bên cạnh đó, chi phí đầu tư cho thẻ thông minh cũng rất lớn và vẫn còn nguy cơ rủi ro. Cho nên, nếu chỉ dùng thẻ thông minh sẽ không thích hợp để xác thực trong điện toán đám mây. Cho nên, nếu chỉ dùng thẻ thông minh sẽ không thích hợp để xác thực trong điện toán đám mây.

1.2.2.2. Kỹ thuật về RFID

Kỹ thuật RFID có liên quan đến hệ thống không dây cho phép một thiết bị đọc thông tin được chứa trong một chip không tiếp xúc trực tiếp mà ở khoảng cách xa, mà không thực hiện bất kỳ giao tiếp vật lý nào hoặc yêu cầu sự nhìn thấy giữa hai thiết bị. Nó cho ta phương pháp truyền và nhận dữ liệu từ một điểm đến điểm khác.

1.2.2.2.1. Nguyên lý làm việc của RFID

Một hệ thống RFID cơ bản có ba thành phần: thẻ, đầu đọc, và một host computer. Thẻ RFID gồm chip bán dẫn nhỏ và anten được thu nhỏ trong một số hình thức đóng gói.

1.2.2.2.2. Ưu điểm

Không cần nhìn thấy đối tượng cũng có thể định danh được đối tượng, có độ bền cao, chịu được hoạt động trong các môi trường khắc nghiệt, việc truy cập không cần tiếp xúc.

1.2.2.2.3. Nhược điểm

Giá cao

Dễ bị ảnh hưởng gây nhiễu

Kết luận:

Mặc dù thẻ RFID có nhiều ưu điểm nhưng nó còn rất nhiều hạn chế như chi phí cao, phải đầu tư cơ sở hạ tầng lớn, gây khó khăn cho người sử dụng, đụng độ đầu đọc cũng như chưa xây dựng được chuẩn hóa cho loại thẻ này. Chính vì vậy, thẻ RFID không thích hợp để sử dụng xác thực trong điện toán đám mây.

1.2.3. Xác thực dựa trên sinh trắc học (biometric)

1.2.3.1. Tổng quan về xác thực theo sinh trắc học

Xác thực dựa theo sinh trắc học là phương thức sử dụng công nghệ như nhận dạng vân tay, võng mạc, khuôn mặt, giọng nói, loại máu, những chi tiết sinh học nhỏ trên cở thể người dùng…

1.2.3.2. Các thành phần trong hệ thống xác thực sinh trắc học

Một hệ thống sinh trắc cơ bản là một hệ thống nhận dạng mẫu để nhận ra một người bằng cách quyết định tính xác thực của một đặc tính sinh học hay hành vi thuộc về người đó. Trong thiết kế một hệ thống sinh trắc, một vấn đề quan trọng đặt ra là xác định cách một người được nhận dạng. Một hệ thống sinh trắc có thể là một hệ thống kiểm tra hay một hệ thống nhận dạng.

1.2.3.3. So sánh các đặc trưng sinh trắc

Một đặc tính sinh học hoặc hành vi của con người có thể được sử dụng như là một đặc trưng sinh trắc trong nhận dạng một người nếu nó có các yêu cầu sau:

- Tính phổ biến
- Tính phân biệt
- Tính ổn định
- Tính thu thập
- Hiệu năng
- Tính chấp nhận
- Khả năng phá hoại

1.2.3.4. Tóm tắt công nghệ xác thực sử dụng các đặc điểm sinh trắc học

Dấu vân tay, khuôn mặt, tiếng nói, chữ ký tay, một số đặc điểm sinh học khác.

Kết luận:

Công nghệ sinh trắc học (Biometric) là công nghệ sử dụng những thuộc tính vật lý, đặc điểm sinh học riêng của mỗi cá nhân như vân tay, mống mắt, khuôn mặt... để nhận diện. Đây được coi là công cụ xác thực người dùng hữu hiệu nhất. Những thiết bị điện tử có khả năng sử dụng dữ liệu sinh trắc học trong thời gian thực để bảo vệ thông tin bí mật của con người.

Tại Việt Nam, công nghệ xác thực bằng sinh trắc học đang đi vào đời sống với các ứng dụng như bảo vệ an toàn các cơ sở quan trọng, phục vụ việc chấm công, điểm danh

trong cơ quan, công ty…Trong tương lai không xa, công nghệ này sẽ có sự phát triển mạnh mẽ, được ứng dụng rộng rãi tại Việt Nam.

Tuy có những ưu điểm như vậy nhưng sử dụng công nghệ sinh trắc học cũng có hạn chế là phải đầu tư cơ sở hạ tầng lớn, hay là gặp khó khăn trong quá trình xác thực khi mà tuổi đã cao, dấu vân tay bị mờ. Hoặc là gặp phải các tác động ngoại cảnh làm tổn thương dấu vân tay, giọng nói, võng mạc mắt, đặc biệt là bị tin tặc với các công nghệ tinh vi có thể lấy được và sử dụng vân tay, giọng nói, hay thiết bị quét võng mạc mắt để đăng nhập trái phép …. Như vậy, nếu chỉ sử dụng công nghệ này sẽ không thích hợp để sử dụng trong điện toán đám mây.

Kết luận chương:

Với các công nghệ xác thực truyền thống như: username/password, Smart card, kỹ thuật radio frequency identification (rfid), Sinh trắc học (biometric) tuy có nhiều ưu điểm nhưng cũng có nhiều hạn chế khi sử dụng các công nghệ này để xác thực trong điện toán đám mây, chẳng hạn như: username/password có thể bị thay đổi hoặc đánh cắp; thẻ thông minh (Smart card) hay thẻ RFID thì phải đầu tư cơ sở hạ tầng lớn, hỏng thẻ; sinh trắc học cũng không an toàn vì tin tặc với các công nghệ tinh vi có thể lấy được và sử dụng vân tay, giọng nói, hay thiết bị quét võng mạc mắt để đăng nhập trái phép.

Chính vì lý do trên, chúng ta có thể thấy rằng xác thực bằng các phương pháp này sẽ không còn phù hợp trong điện toán đám mây.

Với việc sử dụng giải pháp xác thực truyền thống là không an toàn, người sử dụng cần những giải pháp xác thực tốt hơn trong môi trường kinh doanh hiện nay, nhất là trong điện toán đám mây. Một giải pháp xác thực được gọi là tốt và được đánh giá cao khi nó đáp ứng được những yêu cầu chủ yếu sau: Độ an toàn cao, hoạt động liên tục, thuận tiện, chi phí thấp, dễ dàng, thuận tiện cho người sử dụng và sử dụng được trong nhiều hệ thống, khả năng mở rộng và tương thích với các hệ thống khác tốt.

Giải pháp xác thực người dùng sử dụng công nghệ “two factor authentication” đã đáp ứng được những yêu cầu mới về an ninh mạng hiện nay, đặc biệt là trong điện toán đám mây.

Chương 2: NGHIÊN CỨU MỘT SỐ CÔNG NGHỆ XÁC THỰC NGƯỜI DÙNG ỨNG DỤNG TRONG DỊCH VỤ ĐIỆN TOÁN ĐÁM MÂY

2.1. Tổng quan về điện toán đám mây và xác thực người dùng dử dụng điện toán đám mây

2.1.1. Định nghĩa điện toán đám mây

Theo Wikipedia: "Điện toán đám mây (cloud computing) là một mô hình điện toán có khả năng co giãn (scalable) linh động và các tài nguyên thường được ảo hóa được cung cấp như một dịch vụ trên mạng Internet".

2.1.2. Các mô hình triển khai điện toán đám mây

- Đám mây "công cộng"
- Đám mây "doanh nghiệp"
- Đám mây "chung"
- Đám mây "lai"

Kết luận:

Mô hình điện toán đám mây là mô hình mới, chính xác hơn là mô hình ứng dụng và khai thác điện toán mới, được đánh giá là rất tiềm năng và mang lại hiệu quả cao. Hy vọng trong tương lai gần, khác hàng và doanh nghiệp sẽ quen với việc sử dụng các phần mềm và lưu dữ liệu ở ngoài ngôi nhà, văn phòng của mình, ở trên "mây".

2.2. Mô tả công nghệ xác thực hai yếu tố và tích hợp trong điện toán đám mây

2.2.1. Khái niệm

Xác thực hai yếu tố là:

+ Những gì người sử dụng biết - một mật khẩu hoặc số nhận dạng cá nhân (PIN).

+ Những gì người sử dụng có - một đặc tính độc đáo về thể chất (chẳng hạn như một dấu vân tay), hoặc thiết bị (chẳng hạn như một chiếc điện thoại), mà chỉ có những người dùng có quyền truy cập vào.

2.2.2. Hoạt động của giải pháp xác thực hai yếu tố

Bước 1: Người quản trị khi có nhu cầu kết nối vào hệ thống sẽ lấy password OTP

Bước 2: Các thiết bị/dịch vụ/OS nhận được thông tin từ người quản trị nhập vào sẽ gửi yêu cầu xác thực đến OTP Radius Server thông quagiao thức RADIUS.

Bước 3: Trên OTP Radius Server kiểm tra nếu password OTP là hợp lệ thì sẽ phản hồi lại cho thiết bị/dịch vụ/OS biết truy cập này được chấp nhận hay không.

2.2.3. Mật khẩu một lần(One Time Password (OTP))

Để cung cấp xác thực hai yếu tố cho các dịch vụ máy tính và các trang web sử dụng dịch vụ điện toán đám mây, người sử dụng phải dựa trên mật khẩu một lần (One Time Password (viết tắt là OTP)).

2.2.3.1. Cách tạo password và phân phối OTP

Dựa trên đồng bộ hóa thời gian giữa các máy chủ xác thực và khách hàng cung cấp mật khẩu (OTP chỉ có giá trị cho một khoảng thời gian ngắn).

Sử dụng một thuật toán tạo mật khẩu mới được dựa trên một thách thức

2.2.3.2. Cơ chế tạo ra OTP

- OTP dựa trên sự kiện (OTP Event based)
- OTP Challenge Response Based (Thử thách - Hồi đáp)
- OTP dựa trên thời gian thực (OTP Time Based)

2.2.4. Sinh trắc học được sử dụng như là yếu tố thứ hai

Sinh trắc học xác thực sử dụng như một yếu tố xác thực của người dùng cuối, chẳng hạn như dấu vân tay hoặc mống mắt quét để cung cấp xác thực. Các yếu tố sử dụng trong sinh trắc học bao gồm:

- Quét mắt, hoặc mống mắt quét
- Các thiết bị nhận dạng giọng nói xác minh bằng giọng nói của người nói đối với mẫu lưu trữ ngôn luận
- Dấu vân tay sinh trắc học
- Thiết bị nhận dạng hình dạng của tay hoặc lòng bàn tay tương tự có thiết bị

Như vậy, với sự lựa chọn đa dạng các yếu tố xác thực từ các yếu tố xác thực trên, người sử dụng TFA có thể hoàn toàn yên tâm khi đăng nhập vào các đám mây “công cộng”, đám mây “doanh nghiệp”, đám mây riêng, đám mây chung hay đám mây lai vì tính xác thực mạnh mẽ mà nó cung cấp.

2.2.5. Triển khai hai yếu tố xác thực

Bất kỳ một cơ quan, tổ chức, ngân hàng, doanh nghiệp hay một cá nhân nào đó khi xem xét triển khai 2FA trong điện toán đám mây phải lựa chọn giữa một loạt các thiết bị xác

thực dưới đây để phục vụ cho nhu cầu, mục đích của mình. Danh sách sau đây cung cấp có thể không đầy đủ nhưng sẽ đưa ra những mẫu đại diện nhất:

- Thẻ EMV và Reader (EMV Card and Reader)
- Thẻ phần cứng và phần mềm OTP (Hardware & Software OTP Tokens)
- Phần cứng dựa trên PKI Token
- Phần mềm dựa trên PKI Token
- OTP dựa trên SMS
- Danh sách giao dịch số xác thực (TAN Lists)
- Thẻ ma trận

2.2.6. Các mối nguy hiểm của xác thực hai yếu tố

2.2.6.1. Cuộc tấn công Man-in-the-Middle (MITM)

Các cuộc tấn công Man-in-the-Middle (MITM) xảy ra khi người tấn công lừa gạt người sử dụng thiết lập một kênh liên lạc với một máy chủ server hoặc dịch vụ nào đó xuyên qua một ‘rogue entity’. Ở đây, rogue entity chính là hệ thống do hacker điều khiển. Nó được dựng lên để chặn đứng việc liên lạc giữa người sử dụng và server mà không để cho người sử dụng nhận thấy được rằng tấn công đang diễn ra.

Kết luận:

Mặc dù, công nghệ này có thể chiếm đoạt quyền đăng nhập hệ thống để truy cập trái phép và thực hiện những hành vi xấu. Tuy nhiên, việc thực nó thật không hề đơn giản: hacker phải có trình độ kỹ thuật, kinh nghiệm rất cao và tốc độ xử lý rất nhanh để có thể thực hiện hành vi này vì thời gian của mật khẩu một lần tồn tại trong thời gian rất ngắn (thường là 30s hay 60s) cùng với bàn phím rất nhạy. Hoặc hacker phải trang bị một hệ thống tự động hóa toàn bộ để thực hiện hành vi ăn cắp tài khoản. Tóm lại, bảo mật luôn là không hoàn hảo nhưng công nghệ two factor authentication là một công nghệ mới với độ bảo mật cao, cùng với các kỹ thuật hack về công nghệ này chưa phát triển nên trong tương lai gần công nghệ này vẫn có thể đảm bào an toàn và thích hợp để triển khai trong điện toán đám mây.

2.2.7. Ưu điểm và nhược điểm của xác thực hai yếu tố

Ưu điểm:

Tăng cường an ninh: Rất nhiều người chọn mật khẩu có chứa các chi tiết quen thuộc như ngày sinh hoặc một tên con vật cưng mà làm cho nó khá dễ dàng để được đoán. Ngoài

ra một mật khẩu có thể bị mất hoặc quên. Phá mật khẩu thường là dễ dàng cho tin tặc và họ được tiếp cận với nguồn lực hạn chế. Tuy nhiên, hai yếu tố xác thực (TFA) không cho phép các hacker tiếp cận với dữ liệu. Các hacker tốt nhất, có thể tìm ra mật khẩu của người dùng, nhưng họ sẽ không thể xâm nhập hệ thống của người dùng hơn nữa vì các mã được tạo ra duy nhất hoặc in ngón tay mà vẫn hoạt động chỉ trong một thời gian rất ngắn. Nếu không có kiến thức về các mã được tạo ra, bên cạnh đó là không thể đối với kẻ tấn công để có được truy cập.

Giảm nguy cơ đánh cắp dữ liệu: Mất cắp dữ liệu không phải là mới trong thời đại ngày nay. Nhiều tổ chức đã bị thiệt hại đáng kể và giao dịch kinh doanh của họ không thành công do bị mất cắp dữ liệu có giá trị. Việc sử dụng TFA sẽ bảo vệ an toàn hệ thống của các doanh nghiệp, tổ chức hay ngân hàng,… với bảo mật nâng cao, kỹ thuật phức tạp gây khó khăn cho hacker trong việc khai thác các lỗ hổng.

Linh hoạt hơn và năng suất: Hiện nay, một số lượng lớn của các công ty cho phép nhân viên làm việc từ xa từ nơi làm việc của họ, xác thực hai yếu tố đảm bảo rằng chỉ những người dùng có đủ quyền mới được phép truy cập vào cơ sở dữ liệu của công ty. Như vậy, hai yếu tố xác thực giúp người dùng đạt năng suất tốt hơn và tiết kiệm thời gian để đi du lịch hay làm việc an toàn tại nhà hay bất cứ nơi đâu mà không phải lo lắng về dữ liệu của họ đang bị tổn hại hay mất cắp.

Đáp ứng yêu cầu của ngân hàng nhà nước về việc sử dụng cơ chế xác thực đa thành phần trong quản trị hệ thống CNTT đối với các ngân hàng, tổ chức tín dụng.

Sử dụng giải pháp sử dụng mã nguồn mở nên không tốn chi phí bản quyền mà vẫn đảm bảo độ an toàn cao. Ví dụ như giải pháp mã nguồn mở Google Authenticator.

Tận dụng những thiết bị, công cụ sẵn có của hệ thống để tích hợp giải pháp trên.

Chi phí triển khai của thấp. Ví dụ có thể sử dụng điện thoại di động (đa số mọi người đều mang theo bên mình) làm yếu tố xác thực thứ hai.

Nhược điểm:

Một số người thấy bất tiện vì phải đăng nhập hai lần hoặc luôn phải mang theo một vật gì đó làm yếu tố xác thực thứ hai.

Khi mà xác thực hai yếu tố trở nên phổ biến hơn, nhiều khả năng sẽ có nhiều hơn các cuộc tấn công chống lại nó, đó là bản chất của thế giới bảo mật máy tính. Tuy vậy, việc trở nên phổ biến hơn sẽ làm nó trở nên dễ dàng hơn trong việc sử dụng.

Kết luận:

Xác thực hai yếu tố là một hình thức mạnh mẽ hơn xác thực một yếu tố. Thực hiện một giải pháp hai yếu tố để xác thực người dùng trực tuyến đóng một vai trò quan trọng trong cuộc chiến chống lừa đảo trực tuyến. Xác thực hai yếu tố có thể loại bỏ nguy cơ lừa đảo và giảm thiểu các cuộc tấn công trực tuyến. Có vô số các thiết bị hai yếu tố và phương pháp trong thị trường hiện nay, trong đó có mức độ hiệu quả, chi phí và khả năng sử dụng khác nhau. Vì thế các doanh nghiệp, ngân hàng, nhà nước hay người dùng dùng cá nhân, tuy theo mục đích sử dụng sẽ có nhiều lựa chọn khác nhau để đảm bảo an toàn thông tin và các dịch vụ khi sử dụng trong điện toán đám mây.

Xác thực hai yếu tố là một giải pháp hiệu quả cho vấn đề bảo mật trực tuyến ngày hôm nay, nó sẽ ngăn chặn các nguy cơ lừa đảo trực tuyến. Tuy nhiên, việc bảo vệ thiết bị đầu cuối người dùng và giáo dục người dùng cách sử dụng an toàn cũng đóng một vai trò hết sức quan trọng.

Kết luận chương:

Ngày nay, yếu tố xác thực duy nhất, ví dụ mật khẩu, không còn được coi là an toàn trên Internet và trên thế giới ngân hàng. Dễ đoán mật khẩu, chẳng hạn như tên, tuổi, hoặc có thể dễ dàng phát hiện bởi các chương trình hack mật khẩu. Giải pháp hai yếu tố xác thực (Two factor authencation) sử dụng trong điện toán đám mây đã đáp ứng nhu cầu của các tổ chức cung cấp tùy chọn xác thực mạnh cho người sử dụng, linh hoạt, đạt hiệu suất cao cũng như chi phí phù hợp. Trong hầu hết các trường hợp, một mã thông báo phần cứng được trao cho mỗi người dùng cho mỗi tài khoản. Tăng số lượng thẻ thực hiện và chi phí sản xuất và duy trì nó đang trở thành một gánh nặng cho cả khách hàng và tổ chức. Ngày nay, khi mà nhiều khách hàng mang theo điện thoại di động, một lựa chọn khác là cài đặt tất cả các phần mềm xác thực hai yếu tố trên điện thoại di động. Điều này sẽ giúp giảm chi phí sản xuất và số lượng thiết bị thực của khách hàng, đồng thời tăng lợi nhuận cho ngân hàng hay nhà cung cấp dịch vụ,…

Chương 3: NGHIÊN CỨU TÍCH HỢP CÔNG NGHỆ XÁC THỰC HAI BƯỚC TRUY CẬP DỊCH VỤ ĐÁM MÂY RIÊNG IDRAGON CLOUDS

3.1. Điện toán đám mây riêng iDragon Clouds

- Tổng quan
- Khách hàng

- Mô hình triển khai
- Các dịch vụ đám mây iDragon Clouds
- Các giải pháp phần mềm trên nền tảng đám mây iDragon Clouds

3.2. Cổng kết nối dịch vụ đám mây riêng iDragon CloudGates

- Kết nối và truy cập dịch vụ bên trong đám mây riêng.
- Cung cấp cơ chế xác thực người dùng, cung cấp thông tin kết nối đám mây riêng, truy cập dữ liệu và dịch vụ bên trong các đám mây riêng.

3.3. Chương trình minh họa quá trình xác thực sử dụng công nghệ two factor authentication truy cập dịch vụ đám mây riêng qua cổng đám mây iDragon CloudGates

Ngày nay, với những tiến bộ trong phần cứng và phần mềm, điện thoại di động hay máy tính bảng sử dụng đã được mở rộng để gửi tin nhắn, email kiểm tra, liên hệ cửa hàng, v.v tùy chọn kết nối di động cũng đã tăng lên. Sau khi kết nối tiêu chuẩn GSM, điện thoại di động bây giờ có hồng ngoại, Bluetooth, 3G, và kết nối WLAN. Hầu hết người sử dụng đều mang theo điện thoại di động hay máy tính bảng cho mục đích truyền thông, giải trí, làm việc... Một số dịch vụ điện toán đám mây đã tận dụng lợi thế của các tính năng nâng cao của thiết bị di động ví dụ như điện toán đám mây Rồng thông minh iDragon Clouds tại Viện Công nghệ phần mềm và nội dung số Việt Nam (Bộ Thông tin và Truyền thông).

Do đó, bằng cách sử dụng điện thoại di động hay máy tính bảng như một mã thông báo sẽ thuận tiện hơn cho người sử dụng để đáp ứng được với nhiều hệ thống xác thực hai yếu tố.

Trong phần này, em tập trung nghiên cứu, xây dựng và phát triển một hệ thống xác thực hai yếu tố sử dụng giải pháp nguồn mở Google Authenticator. Google Authenticator đã có sẵn trên thư viện app của Android hay iOS :

Phần mềm có thể sử dụng một ứng dụng điện thoại di động hoặc máy tính bảng được cài hệ điều hành Androi hoặc iOS để tạo ra thời gian chính xác với mật khẩu một lần (OTP) cùng với mật khẩu của người dùng để đăng nhập. Giải pháp nguồn mở Google Authenticator trên ứng dụng di động hoạt động với nhiều cấu hình khác nhau. Điều này cho phép bất kỳ nhà phát triển để sử dụng ứng dụng Google với hệ thống xác thực ứng dụng riêng của họ. Nhà cung cấp dịch vụ đám mây chỉ cần phát triển các thành phần của máy chủ

để làm cho nó làm việc với các ứng dụng web. Giải pháp nguồn mở Google Authenticator sử dụng một tiêu chuẩn mở HMAC dựa trên One-Time Password (HOTP).

Trong trường hợp người sử dụng không đăng nhập được bằng mã xác thực tạo ra trên điện thoại thông minh hay máy tính bảng, hoặc để quên chúng ở nhà, mất trộm hay hư hỏng nặng… thì người dùng có thể sử dụng một trong những mã xác minh dự phòng được tạo ra một lần và duy nhất khi đăng ký tài khoản.

Kết luận:

Trong chương này, em đã tập trung vào việc phân tích, thực hiện các phương pháp xác thực hai yếu tố sử dụng điện thoại di động thông minh hoặc máy tính bảng được cài đặt hệ điều hành Android hoặc iOS. Phương pháp này đã được thực hiện thành công và thử nghiệm, và thể hiện được mạnh mẽ và an toàn trên nền tảng đám mây Idragon của Viện công nghệ phần mềm và nội dung số Việt Nam. Hệ thống này đảm bảo an toàn và thân thiện với người sử dụng. Trong tương lai, hệ thống này sẽ phát triển mở rộng và đa dạng hơn bao gồm một giao diện thân thiện với người dùng hơn và mở rộng các thuật toán để làm việc trên Blackberry, Palm, và điện thoại di động dựa trên Windows cùng với việc sử dụng Bluetooth và tính năng mạng WLAN trên điện thoại di động để bảo mật tốt hơn và rẻ hơn.

Kết luận chương:

Giới thiệu giải pháp điện toán đám mây nguồn mở iDragon.

Xây dựng chương trình xác thực hai yếu tố sử dụng điện thoại di động thông minh hoặc máy tính bảng được cài đặt hệ điều hành Android hoặc iOS. Phương pháp này có ưu điểm là điện thoại thông minh hay máy tính bảng không cần có kết nối mạng internet mà vẫn cung cấp mã số (code) để người dùng xác thực, thuận tiện cho người sử dụng làm việc ở mọi lúc, mọi nơi, an toàn và dễ sử dụng.

III. KẾT LUẬN

1. Những kết quả đã đạt được của luận văn

- Luận văn đã khái quát, phân tích, đánh giá các công nghệ xác thực truyền thống. Phân tích ưu nhược điểm của các công nghệ này. Phân tích công nghệ nào thích hợp để sử dụng trong điện toán đám mây.

- Luận văn cũng cung cấp những kiến thức tổng quan về điện toán đám mây.

- Phân tích, đánh giá công nghệ xác thực dùng trong điện toán đám mây, tập trung phân tích công nghệ Two factor authencation sử dụng trong điện toán đám mây. - Giới thiệu giải pháp điện toán đám mây nguồn mở iDragon.

- Xây dựng chương trình minh họa quá trình xác thực hai yếu tố sử dụng điện thoại di động thông minh hoặc máy tính bảng được cài đặt hệ điều hành Android hoặc iOS. Hệ thống này sử dụng giải pháp sử dụng giải pháp nguồn mở Google Authenticator và tích hợp vào đám mây Idragon của Viện công nghệ phần mềm và nội dung số Việt Nam.

2. Hướng nghiên cứu tiếp theo

Do thời gian và điều kiện cá nhân còn hạn chế, nên vấn đề nghiên cứu về "Nghiên cứu công nghệ xác thực người dùng ứng dụng trong quản lý truy cập dịch vụ điện toán đám mây" trong khuôn khổ của luận văn này chỉ tập trung nghiên cứu công nghệ Two factor authencation trong điện toán đám mây. Vì vậy, những nghiên cứu tiếp theo về vấn đề này có thể tập triển khai theo các hướng như sau:

- Tìm hiểu thêm những công nghệ xác thực khác sử dụng trong điện toán đám mây.

- Xây dựng phần mềm hoàn thiện để sử dụng các công nghệ xác thực sử dụng trong điện toán đám mây.

- Xây dựng chính sách về tính chi phí khi sử dụng các công nghệ xác thực trong điện toán đám mây.